ANWENDERBERICHT

Signifikanter Schutz gegen Kryptotrojaner durch E-Mail Security Gateway und Sandbox

DOKOM21 ist 1997 als City-Carrier aus den Dortmunder Stadtwerken ausgegründet worden. Heute deckt der Netzbetreiber ein breites Service-Spektrum ab, in welchem der Rechenzentrumsbetrieb mit Colocation- und Hosting-Angeboten, Dienste für IT-Security und Mobilfunk wichtige Standbeine bilden. Über die Jahre weitete der Netzbetreiber und Provider sein Anschlussgebiet von Dortmund auf die Nachbarstädte und bis in den Märkischen Kreis sowie nach Essen aus.

Einer der größten Kunden ist die Dortmunder Stadtwerke AG (DSW21) mit ihren Tochterfirmen. Die knapp 4.000 Mitarbeiter der Unternehmensgruppe erwarten IT-Sicherheit auf höchstem Niveau, wozu DOKOM21 Sicherheitslösungen wie Firewalls, Web- und Mail-Filter sowie IDP (Intrusion Detection & Prevention) bereitstellt.

Im Frühjahr 2016 verbreiteten sich die Kryptotrojaner Locky, TeslaCrypt und Petya rasant. Experten zählten damals in den Hochzeiten von Locky 5.000 Infizierungen pro Stunde in Deutschland. „Die akute Gefährdung durch Ransomware machte es notwendig, unsere Infrastruktur mit einem höheren Funktionsumfang besser abzusichern. Als solide Basis hatten wir eine klassische Firewall-Lösung von Fortinet im Einsatz. Die Frage war, wie stellen wir vor allem E-Mail-Sicherheit auf höchstem Niveau her“, erinnern sich Stefan Skuballa (Bereichsleiter Betrieb und Datenverarbeitung) und Torsten Bär (Systemadministration und Sicherheit) bei DOKOM21. Diese Überlegungen waren die Grundlage für eine umfangreiche Marktanalyse.

Erweiterung der Fortinet-Firewall mit FortiMail Security Gateway und FortiSandbox

Das Haupteinfallstor für Schad-Software sind E-Mails, welche Schadcode entweder in Anhängen und/oder in Weblinks auf Malware enthalten. Herkömmliche Virenscanner nutzen die Signaturen bekannter Schädlinge, um Infektionsgefahren durch Viren, Würmer und Trojaner zu erkennen. In Fällen der sogenannten Zero-Day-Attacken sind die Angriffe jedoch neu oder erscheinen durch Mutation des Codes wie neu. Bis die entsprechende Signatur und damit wirksamer Schutz bereitgestellt wird, vergeht wertvolle Zeit. Und diese Schutzlücken treten leider immer häufiger auf. Abhilfe in solchen Situationen bieten FortiMail und FortiSandbox.

“Einige Eindringlinge hat FortiSandbox bereits registriert und abgefangen. Durchgekommen ist noch kein Angreifer. Das ist der entscheidende Parameter. Jeder Tag, den wir und die DSW21-Gruppe unbeschadet überstehen, zeigt, dass die Fortinet Security Fabric ganze Arbeit leistet.”

– *Stefan Skuballa, Bereichsleiter Betrieb und Datenverarbeitung, DOKOM21*

Am Ende der Marktsondierung entschied sich DOKOM21 für eine Kombination aus Fortinet-Technologie und IT-Dienstleistungen von GORDION. Das IT-Consulting- und Systemhaus ist seit 2003 Partner von Fortinet und hat bereits die Firewall installiert, welche das Netzwerk absichert. „In der Auswahlphase haben wir einen Proof of Concept durchgeführt, um alle Komponenten-Eigenschaften besser zu verstehen. Dabei hat uns GORDION kräftig unterstützt“, berichtet Stefan Skuballa. „Schnell stand als beste Lösung fest, die erfolgreiche Fortinet-Firewall zu erweitern. Und unser IT-Partner GORDION weiß, was da zu tun ist.“

Der Platinum Partner von Fortinet baute die Firewall in Richtung Fortinet Security Fabric aus. In einem intelligenten Framework interagieren unter anderem die Next Generation Firewall FortiGate, das E-Mail Security Gateway FortiMail sowie FortiSandbox und bieten so Advanced Threat Protection – einschließlich durch die FortiSandbox initiierter Updates. Ein Vorteil, der bei Komponenten von Drittanbietern nicht gegeben ist.

FortiMail fungiert als E-Mail Security Gateway und prüft ein- und ausgehende E-Mails. Bei DOKOM21 sind dies 3.000 E-Mails pro Stunde. Verdächtige Nachrichten leitet FortiMail an FortiSandbox weiter. Diese checkt in mehreren Stufen auf Anomalien, welche auf Schadcodes hindeuten. In der höchsten Prüfungsstufe führt sie in integrierten Virtual Machines (VM) verdächtige Links oder Anhänge gezielt aus. Bei diesem Test zeigt sich final, ob Schadcode aus dem Internet nachgeladen wird und mit welchen IP-Adressen die Malware kommuniziert.

Das Setup wird durch das Monitoring- und Reporting-Tool FortiAnalyzer ergänzt. Es erfasst die Logging-Daten, bereitet diese auch grafisch auf und gibt so einen Einblick in etwaige Bedrohungen – dank des integrierten Indicator of Compromise Service (IOC). „Funktionsumfang und -weise der jetzigen Lösung suchen ihresgleichen, sie bilden eine perfekte Einheit. So identifiziert FortiSandbox Bedrohungen und gibt als Bestandteil der Fortinet Security Fabric automatisiert schützende Informationen an das Security Gateway FortiMail und die Next Generation Firewall FortiGate. Die Integration in dieser Tiefe gelingt nur mit Fortinet“, erklärt Oliver Lindlar, Mitglied der Geschäftsleitung (Vertrieb & Marketing) von GORDION.

Schneller und sicherer E-Mail-Verkehr

Ausgehend vom Proof of Concept integrierte GORDION die FortiMail/FortiSandbox-Lösung bei DOKOM21 im Rahmen der Security Fabric. Nach der erfolgreichen Testphase und parallelen Schulung der Mitarbeiter wurde in den Live-Betrieb umgeschaltet. In rekordverdächtigen drei Monaten erhöhten DOKOM21 und GORDION signifikant die Netzwerksicherheit in der DSW21-Gruppe. „Die E-Mail-Kommunikation läuft ganz normal und wird nicht durch unser neues Sicherheitssystem gestört. Einige Eindringlinge hat die Sandbox bereits registriert und abgefangen. Durchgekommen ist noch kein Angreifer. Das ist der entscheidende Parameter. Jeder Tag, den wir und die DSW21-Gruppe unbeschadet überstehen, zeigt, dass die Fortinet Security Fabric ganze Arbeit leistet. Wenn nichts passiert, ist das eine sehr gute Nachricht“, betont Stefan Skuballa.

Eckdaten

Kunde: DOKOM21 - DOKOM Gesellschaft für Telekommunikation mbH

Branche: Informations- und Kommunikationstechnik

Standort: Dortmund

Vorteile

- FortiMail und FortiSandbox bilden eine perfekte Schutzeinheit für den E-Mail-Verkehr
- Fortinet-Komponenten fügen sich nahtlos zu einer tief integrierten Lösung
- Erweiterung der Firewall zur Fortinet Security Fabric bietet höchstes Sicherheitsniveau
- Übertragung der etablierten Sicherheitsmechanismen auf den Internet-Verkehr

Und Torsten Bär ergänzt: „Bei tausenden von E-Mails, die pro Stunde in der Gruppe eingehen, kontrolliert die Sandbox, ohne dass signifikant verzögert zugestellt wird – weil FortiMail und FortiSandbox perfekt miteinander harmonieren.“

Schadcodes können binnen Stunden mutieren. Die Fortinet Security Fabric, unter anderem bestehend aus FortiGate Next Generation Firewall, FortiMail E-Mail Security Gateway und FortiSandbox bietet höchstes Sicherheitsniveau und zeigt, wie der Hersteller im Kopf-an-Kopf-Rennen mit den Cyber-Kriminellen gegenhält.

FORTINET

www.fortinet.com

May 21, 2019

380652 - DOKOM Case Study